NOTICE: This publication is available digitally on the HQ AFMC WWW site at: http://afmc.wpafb.af.mil. If you lack access, contact the Air Force Publishing Distribution Center (AFPDC).

This supplement applies to the US Air Force Reserve units and members.

SUMMARY OF REVISION

This supplement has been extensively revised and will require thorough review.

AFI 31-401, 1 Jan 1999, is supplemented as follows:

1.2. Installation and Headquarters Information Security Program Managers (ISPMs) implement and oversee the Information Security Program for the purpose of protecting collateral classified information. Other program infrastructures, independent of the ISPM, are established for protecting classified information in Special Access Program (SAP) and Sensitive Compartmented Information (SCI) arenas. The ISPM provides support to these areas when requested by appropriate authority within those channels. The ISP is an installation-wide program that provides services to all organizations, both permanent and tenant. To ensure a comprehensive and effective program, AFI 31-401 prescribes one ISPM per base and this title and authority is assigned to the Chief of Security Forces (CSF). There are some current exceptions to this policy in AFMC wherein the Director/Chief of Acquisition Security/Program Protection is assigned the ISPM role because of the large number of acquisition programs formerly assigned to product centers. The diminishing number of these programs now makes assignment of the ISPM function under the CSF the desired structure.

1.3.4. The ISPM is responsible for providing standard services, as defined in information security program directives, to all organizations on the base. Organizations who can demonstrate that it is impractical to receive local ISPM support must submit a request for waiver to permit duplication of this support function IAW AFI 25-201, *Support Agreement Procedures*.

1.3.4.4. (Added) ISPMs below MAJCOM level supplement this directive and provide an electronic copy to HQ AFMC/SFXP.

1.3.5.1. Security manager duties in Air Force organizations are performed by military or DoD civilian employees. The role of security manager is generally assigned as an additional duty, but organizations who generate, process or store large amounts of classified may require a fulltime GS-080 Security Specialist to perform these duties.

1.3.6.2. The servicing ISPM provides assistance to security managers as required in the development of their security operating instructions.

1.4.1.1. (Added) The HQ AFMC ISPM staff will conduct a program review of each installation level ISPM security program at intervals no greater than every three years as budget allocations permit. HQ AFMC/SF will publish a schedule of planned program reviews in September for the following FY quarters. These reviews cover protection of collateral classified only. SAP and SCI classified information security programs are reviewed within their respective channels.

1.4.1.2. (Added) The Program Review Team Leader will outbrief the CC/CV at the level of command above the ISPM at product, logistics and test centers upon completion of the review. The Team Leader will outbrief the site/organization commander, as appropriate, in all other cases. A final report will be provided within 10 working days of completion of the review.

1.4.2. Program reviews are assessments of elements of the information, personnel, industrial, safeguarding NATO and program protection security programs for policy compliance and program effectiveness. At centers, these reviews should be conducted in conjunction with reviews by other functional security areas whenever possible to minimize impact on the organization visited. An ISPM annual program review can be counted as one semiannual self-inspection.

1.4.2.1. (Added) Program reviews are not rated. They serve two primary purposes: (1) identify benchmark processes/products within a program for crossfeed to all serviced organizations, and (2) identify problem areas within a program and recommend corrective action. Program reviewers are encouraged to use a random sampling method; but the examination must be sufficiently thorough to determine the overall effectiveness of the program.

1.4.2.2. (Added) Commanders and staff agency chiefs review Information Security Program Review Reports and implement corrective actions as soon as possible. This review is documented by the commander/staff agency chief endorsement to the report, with the report then filed by the security manager. Formal responses to program reviews are generally not required; however, corrective actions to remedy serious deficiencies are documented and reported according to local policy. If required by the servicing ISPM, the written response must be submitted within 30 days of notification.   Keep copies of program review reports IAW records management directives. As a minimum keep a copy until the next program review report is received.

1.4.2.3. (Added) To provide maximum flexibility consistent with a visible program, ISPMs may extend the interval between program reviews to two years when either of the following conditions exist and the delay will not affect program effectiveness. The decision to extend the frequency is reserved exclusively for the ISPM.

1.4.2.3.1. (Added) The organization visited has relatively small classified holdings and results of other visits or inspections reflect the unit or activity has a strong information security program.

1.4.2.3.2. (Added) The program review visit requires ISPM travel and TDY funding and budgetary constraints necessitate delaying the program review.

1.5.1.1. HQ AFMC/CV, and other commanders, Program Managers and 2-Ltr Staff Agency Chiefs who report directly to the HQ AFMC Commander, are delegated this authority.

1.5.1.2.1. Within AFMC this means 2-Ltr Directors or Staff Agency Chiefs or higher at all levels of command and commanders of all other subordinate activities and detachments.

1.5.2.3. (Added) The ISPM at HQ AFMC and AFMC Centers are responsible for policy and oversight of NATO security at their level.

1.6.1. HQ AFMC/SF is the approval authority for waivering requirements established in this supplement. Submit requests through the servicing ISPM to HQ AFMC/SF.

1.6.2. (Added) Use AF Form 116, **Request for Deviation from Security Criteria**, to document all deviations. Consolidate multiple deviations caused by a single deficiency on one AF Form 116.

1.6.3. (Added) The responsible activity must implement supplemental controls/compensatory measures for all temporary and permanent deviations. Activities may not use blanket waivers for several different deficiencies.

1.6.4. (Added) The responsible/owning activity commander or two letter staff agency chief signs the 116 and submits the request to the servicing ISPM. ISPMs at all levels approve/disapprove waivers to policies contained in their implementing directives. Requests for waivers to DoD 5200.1-R requirements are forwarded through ISPM channels to the ASD(C3I) for approval/disapproval. ISPMs at each level below the approval authority review the request and add their concurrence/nonconcurrence with comments. Activities may submit three kinds of requests:

1.6.4.1. (Added) Temporary deviations (waivers) for 1 year or less. (Waiver: The approved continuance of a temporary condition that varies from an Information Security Program requirement.)

1.6.4.2. (Added) Permanent deviations (exceptions) for a 2 year period. (Exception: The approved continuance of a non-correctable condition that varies from an information security program requirement.)

1.6.4.3. (Added) Technical deviations (variances) for an indefinite period. (Variance: The continuance of a nonstandard condition, which technically varies from an information security program requirement, but provides essentially the same level of protection.)

1.6.6. (Added) Supplementary Controls/Compensatory Measures compensate for the specific vulnerability created by the deficiency. These controls/measures may cover:

1.6.6.1. (Added) Continuous protection by cleared guard or duty personnel.

1.6.6.2. (Added) Random inspection by cleared guard or duty personnel as prescribed in DoD 5200.1-R, Section 4

1.6.6.3. (Added) An IDS with response capability as prescribed in DoD 5200.1-R, Section 4.

1.7.2. See paragraph 9.2.7(Added) and Attachment 4, A4.6.4 this supplement. ISPMs must continually strive to reduce cost and improve performance. ISPMs develop cost and performance measurements to evaluate their functional area business processes and track process changes to determine their impact on cost and effectiveness.

1.8.1. (Added) Servicing ISPMs are responsible for forwarding reports involving collateral classified information. When these incidents involve SCI or SAP information, the servicing ISPM coordinates with the SSO or SAP office exercising oversight to ensure they are aware of the incident. It is then the responsibility of these SCI/SAP offices to forward the appropriate report through their respective program channels.

2.1.2.3. Organizations submit requests for delegation of original classification authority through the servicing ISPM office.

2.1.2.5. (Added) OCA is delegated to the position. Anyone legally assuming a designated OCA position during the temporary absence of the formally assigned occupant also assumes the OCA.

2.1.2.6. (Added) An individual occupying a position designated OCA cannot further delegate that OCA.

2.1.3. See attachment 1 for a listing of AFMC positions with original classification authority (OCA).

2.3.1. Send an information copy of the challenge through the servicing ISPM to HQ AFMC/SF.

2.3.2. Send an information copy of the challenge through the servicing ISPM to HQ AFMC/SF.

2.3.3. In all instances of challenges alleging underclassification, safeguard the information at the higher level of classification pending final determination. In all instances of challenges alleging overclassification, safeguard the information at the assigned level until the challenge is resolved.

2.4.2.4. (Added) HQ AFMC/SFXP; Building 266, Room N208; 4225 Logistics Ave, Wright-Patterson AFB OH 45433-5760.

2.4.3. Forward an electronic copy to HQ AFMC/SF within 90 days of the publication of this supplement.

2.4.5. (Added) See attachment 2 for additional guidance.

3.1. This authority cannot be further delegated.

3.3.1. Normally, the 11 CS/SCSR (MDR) forwards MDRs involving collateral classified information directly to the ISPM office servicing the OCA involved. When the 11 CS/SCSR cannot readily determine the appropriate OCA, they forward the MDR to HQ AFMC/SF for further distribution determination. HQ AFMC/SF forwards the MDR to the servicing ISPM with distribution instructions and a suspense. This suspense will normally be 10 working days after receipt. The servicing ISPM provides classification management assistance as requested by the OCA conducting the MDR. MDRs involving SCI or SAP information are handled through those program channels.

4.8. (Added) The absence of "NOFORN," or equivalent markings is not authority for any release to a foreign government, representative thereof, or international organization. This applies to classified national security information and unclassified controlled information, but not to information approved for public release. Contact the designated Foreign Disclosure Office for applicable Delegated Disclosure Lists (DDL).

4.9. (Added) The last page of a document will be considered its back cover unless there is a clearly discernible separate page serving as the cover. Mark the back cover as required in the basic directive.

4.10. (Added) Mark file folders containing classified information on the top and bottom of the front and back of the folder with the highest level of classified material contained therein.

5.6.1.2. Requests for access must be signed by a Commander, Special Program Office Director, or 2-Ltr Staff Agency Chief/Director or higher, and be submitted 120 days prior to required access. This permits time for requesting and completing the appropriate background investigation.

5.7. Servicing ISPMs must incorporate visitor control policies and procedures in their local supplement to this directive. These must, as a minimum, define local processes for sending and receiving visit requests, evaluating visit requests, controlling visitors during the visit, tracking the visit to ensure timely departure of visitors, and maintenance of visitor record files. Visit records involving foreign national access to classified or controlled unclassified information must be maintained for a minimum of two years following expiration of the visit or as specified in AFMAN 37-139, *Records Disposition Schedule*. This requirement does not supplant, mitigate or otherwise impact foreign disclosure policies/requirements regarding foreign national visitors.

5.7.1.5. (Added) Unless otherwise specified, the visit request will, as a minimum, include the name and citizenship of the visitor, the visitor's organization and telephone number, certification of the visitor's clearance and any special access authorizations required for the visit, the name of person(s) to be visited, and the purpose and date or period of the visit. AF Form 97 can be used for providing visit notices.

5.10.1.1.1. This includes communications centers and command posts.

5.10.1.6. (Added) Commanders or staff agency chiefs establish TSCAs only when mission dictates, and disestablishes them when no longer required or after 12 months of no receipt, generation or storage of material. Provide written notice of TSCA establishment and closure to the local Information Management Office, when appropriate, and the servicing ISPM. Send a copy of each TSCO and alternate's written appointments to the same offices. Ensure TSCO and alternates attend training provided by the servicing ISPM.

5.13.2. All AFMC General Officers may take Secret and Confidential classified national security information to their home for work purposes provided they reside on a base with an access controlled perimeter and have an approved GSA security container in their residence. The combination to the residence container must be stored in an approved GSA container within the Commander's work center to permit retrieval of the container's contents in the event of an emergency. This authorization does not apply to caveated information such as SCI, SAR, NATO, etc. In all other cases submit requests through the servicing ISPM office to HQ AFMC/SF. The servicing ISPM reviews the request and recommends approval/ disapproval. HQ AFMC/CC has delegated final approval authority for these requests to AFMC/SF.

5.14.1. Cargo security cages or rooms used for temporary storage of classified material must have an intrusion detection alarm operating when attendants are not present. Servicing ISPMs must review and approve these areas prior to their establishment.

5.14.2. "Controlled" means the continual presence of government military or civilian personnel in such proximity as to allow observation and controlling of access to the security container, or the area is monitored by an approved alarm system.

5.15.1. Activities hosting classified meetings will coordinate their security plan with the servicing ISPM. As a minimum, this plan should contain the meeting title, its location, purpose, classification level (if permitted), identity of the responsible security manager, and a statement of who (organization or title) approved the meeting. Also, the plan must address visit request and clearance verification procedures prior to attendee arrival, an assessment of acoustical security controls required during the meeting (e.g. perimeter guards), access controls at the meeting entry point, policy on introducing and utilization of electronic or photographic devices in the meeting room, storage of classified materials (exhibits/docu-

ments) before, during and after the meeting, policy/procedures for note-taking during classified portions of the meeting, and communications/destruction/transmission procedures for those requiring these services during or after the meeting. The plan is not limited to these areas alone and may be expanded as determined locally.

5.15.2. The servicing ISPM ensures security requirements are met by coordinating on all construction plans and procedures for secure conference rooms and by conducting a physical security survey upon completion of construction. All issues regarding EMSEC or TSCM requirements for these rooms are the responsibility of SC and OSI respectively. ISPMs shall maintain a listing of all approved secure conference rooms for customers they service.

5.15.4. Servicing ISPMs review these requests to ensure all security requirements are satisfied and provide formal concurrence/nonoccurrence with the final security plan.

5.18.1. Submit requests to use alternative or compensatory security controls in protecting classified national security information to HQ AFMC/SF for approval/disapproval. In emergencies, when there is no time to first submit a request, controls are applied as deemed necessary and the request is submitted as soon as possible thereafter. This process does not replace or obviate the requirements of DoD 5200.1-R, paragraph 1-401 regarding the submission of waivers.

5.20.2. Paragraph 5.18.1, this supplement, applies when ISPM approval is required.

5.20.4. (Added) The installation commander, in concert with the servicing ISPM and base civil engineer, approves storage of classified national security information in open or unattended storage areas. This includes secure rooms on base, and off base when in the local area and under government control. The installation commander may delegate this approval authority to the servicing ISPM by incorporating such delegation into local supplementation to this directive. The base civil engineer confirms construction of the secure room is IAW DoD 5200.1-R, Appendix G. Before these areas are approved, the using commander, director or staff agency chief submits to the approving authority a written plan for utilization of the secure room, to include security controls employed to provide adequate safeguarding protection and positive entry control to the storage area. The servicing ISPM reviews this plan for accuracy and thoroughness and recommends concurrence/nonconcurrence to the approving authority. See Appendix G, DoD 5200.1-R for construction standards and procedural requirements.

5.20.5. (Added) The purpose of a secure room is to open store classified material when the size and nature of the material, or operational necessity, make the use of General Services Administration (GSA) approved containers or vaults unsuitable or impractical. Secure rooms are never approved solely for the purpose of operational convenience or in lieu of obtaining and using otherwise appropriate GSA-approved containers. In addition, secure rooms are approved to meet a specific operational requirement and only classified national security information relative to that specific requirement should be stored in the approved room. Users of secure rooms must ensure their operational procedures comply with the spirit and intent of this purpose and avoid expedient approaches which reduce protective measures or increase the possibility of compromising classified national security information.

5.20.6. (Added) All structures designated as secure rooms after 20 Nov 96, or new secure rooms constructed after 20 Nov 96, and storing SECRET material/information, which are not continuously occupied or guarded, will be alarmed. Secure rooms approved prior to 20 Nov 96 are exempt from this requirement; however, programming action to fund alarms for these rooms must be pursued when feasible and must be included in any modification or rehabilitation plans. This "grandfathering" provision only applies to the current program, project or activity that necessitated establishment of the secure room. It

doesn't apply to follow-on unrelated programs, projects or activities. Secure room certification is not indefinite and is applicable only for the duration of a program, project or activity and terminates upon completion of the requirement. Install and operate alarm systems IAW DoD 5200.1-R, Appendix G; AFI 31-209; and AFH 31-223, paragraph 10. Minimum system requirements are described in DoD 5200.1-R, Appendix G, Section B, paragraph 5. Submit waivers for alarm requirements to HQ AFMC/SF, through the servicing ISPM, following procedures contained in paragraphs 1.6.1. through 1.6.6.3. above.

5.20.7. (Added) Servicing ISPMs maintain records of all secure rooms to include the specific location of the room, certification of compliance with construction requirements, and approval for the current occupant to operate the secure room. Provide the following information to HQ AFMC/SFXP NLT 31 Jan of each calendar year: Number of secure rooms on the installation, number alarmed, number established as long term and number established as short term. Long term is defined as greater than 12 months. ISPMs develop local procedures to establish this baseline and track compliance.

5.21.3. (Added) When not attended or used, keys providing access to SECRET or CONFIDENTIAL information shall be secured in a GSA approved security container, or in a non-GSA approved container constructed of at least 20-guage steel, or material of equivalent strength, and having a built-in GSA approved combination lock or high security key operated padlock.

5.21.4. (Added) Keys shall not be removed from the premises, and both keys and locks will be audited monthly. The audit is documented using AF Form 2427, **Lock and key Control Register**.

5.25. Any 080 security specialist can perform preventive maintenance inspections on approved GSA security containers as required by TO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Classified Storage Containers*. The inspection is conducted following instructions in paragraph 7 of the TO. Record the inspection on AFTO Form 36, **Maintenance Record For Security Type Equipment**.

5.28.2. Reductions in classified holdings is a continuing key objective within the Air Force and AFMC aggressive support of that objective is the basis for this requirement. Servicing ISPM program implementing directives will establish such processes as are necessary to ensure an ongoing effort throughout the organizations they service to achieve reductions in classified holdings. These processes will be used by the ISPM during program reviews as a starting point for evaluating management of retention of classified material within the organization. Other considerations might include visible organizational policies regarding the reducing of classified holdings, or changes in type and level of activity within the organization which impact the generation of classified documents or material or the amounts routinely received. The number of shredders available, along with education in their desired use and ease of access may also contribute to reduction of classified holdings.

5.28.3. The second Friday of March is the annual clean-out day for AFMC Centers and Staff Agencies. Another date may be chosen if there are compelling local requirements.

5.29.1. The installation commander is responsible for ensuring an adequate local destruction capability exists to dispose of classified material. As a means of consolidating local destruction requirements installation commander may establish a central destruction activity to dispose of classified material for agencies supported. Actual destruction of classified material remains the responsibility of the user activity.

5.29.2.2. When a record must be kept of destroyed Secret or Confidential materials, choose from AF Form 310, AF Form 145 or AF Form 1565.

5.29.2.6. (Added) For a listing of National Security Agency (NSA) evaluated and approved destruction devices see Annex B to NTISSI No. 4004. You may request a copy of this document by writing to NSA

Media Destruction, Maryland Procurement Office, 9880 Savage Road, Ste 6718, Fort Meade MD 20755-6718.

5.30.1. Paragraph 5.18.1(Added), this supplement, applies.

6.7.1.2. As a minimum, couriers must have verbal authorization to hand-carry classified material outside their normal work areas. This approval alone is sufficient when the courier remains within the confines of an access controlled installation perimeter and does not pass through an entry/exit personnel control point. Personnel hand-carrying outside of work areas must use an envelope, folder, or other closed container to prevent loss or observation of the material. Appropriate cover sheets for classified must also be used.

6.7.1.3. (Added) Servicing ISPMs are authorized to approve the overseas hand-carrying of classified information aboard commercial passenger aircraft.

6.8. Use DD Form 2501 when handcarrying within the local area and the courier is required to pass through a manned check point or entry point. DD Form 2501 is carried only when handcarrying classified. Otherwise, the completed form is secured within the issuing organization. Use a courier letter when handcarry will be outside the local area. The boundaries of the local area are determined by the servicing ISPM.

7.2.1.1. (Added) HQ AFMC/LGSW assigns nicknames and annually surveys all OPRs of current nicknames to validate, confirm or cancel sponsor information.

7.2.1.2. (Added) HQ AFMC staff agencies request a nickname through the HQ AFMC/LGSW web page at *http//www.afmc.wpafb.af.mil/HQ-AFMC/LG/lgs/milgov/project.htm*.

7.2.1.3. (Added) Field activities submit unclassified requests, including all necessary information, via e-mail or letter to the HQ AFMC functional OPR. Upon concurrence, the HQ AFMC OPR sends the request to HQ AFMC/LGSW.

7.2.1.4. (Added) Upon receipt of nickname assignment, the HQ AFMC OPR notifies all interested activities of nickname assignments and HQ AFMC/LGSW of project completion or termination of nickname need.

7.2.1.5. (Added) HQ AFMC/LGSW sends information regarding the nickname assignment and its related meaning to OPRs on a need-to-know basis.

8.1. Commanders and Staff Agency Chiefs must have active training programs. Servicing ISPM policies must include the requirement for organizations to develop and implement a local training plan to ensure effective training of all assigned personnel. The plan must outline the type of training, frequency required, subjects to be presented at each session, and how the training will be accomplished. Use of locally developed software programs for presenting the training via automated information systems is the most desired approach. A sample-training plan is provided at Attachment 3. ISPMs are encouraged to invite OPRs for other security disciplines, such as OPSEC, COMPUSEC and Counter Intelligence (CI), to include their training in the ISPM schedule. This would minimize the training footprint on each serviced organization and show the correlation of these security disciplines.

8.2. All training must be documented IAW applicable DoD/AF directives or as locally determined. This includes the categories of training described in DoD 5200.1-R, Chapter 9, as Initial, Special Requirements, Others and Recurring and Refresher Training. As a minimum, one time training documentation is retained as long as the employee is performing the duties which mandate the training. Recurring training documentation, as a minimum, is retained for the current and preceding calendar year. Documentation

methodology must allow tracking of the training to determine date of training, subject areas covered, identity of attendees and percentage of the target group actually receiving/completing the training. Procedures must be in-place to identify, and provide timely make-up for those missing regularly scheduled training.

8.2.1. (Added) The goal is to automate all training to the extent that trainees participate from their work locations and at their own pace in order to minimize trainee time away from their work areas. ISPMs are encouraged to pursue local development of computer based training programs and to provide a copy of their successful products to HQ AFMC/SFXP. HQ AFMC/SFXP will serve as a clearing point for these products and cross feed them to all ISPMs.

8.7.2.2. Servicing ISPMs conduct initial and refresher Security Manager Training following the subject areas listed in DoD 5200.1-R, paragraph 9-303 and other areas as deemed appropriate. As a minimum, new security managers will receive initial training within 60 days of being assigned as security manager. Persons being re-assigned to security manager duties, after not having performed those duties in the preceding 36 months, should be trained as new security managers. The ISPM conducts Security Manager Meetings periodically throughout the year for purposes of addressing program issues and to inform security managers of new or changing program policies and procedures. ISPMs forward a copy of the meeting minutes to HQ AFMC/SFXP within 30 days following the meeting, and maintain record copies of minutes for the current and previous year.

8.9. Because of the volume of information to be covered, Recurring and Refresher Training should, as a minimum, be presented in semi-annual sessions. Quarterly sessions are recommended for maximum motivational and retentive effect. A sample training plan is presented at Attachment 3.

8.12. Servicing ISPMs will evaluate training effectiveness in organizations during program reviews.

9.1.3. Security incidents involving classified national security information in automated information systems are reported to the servicing ISPM for processing IAW with this supplement.

9.2.3. (Added) The servicing ISPM will notify HQ AFMC/SFXP by the end of the next duty day following discovery of these incidents.

9.2.7. (Added) The installation ISPM must submit the Security Incident Data Report to HQ AFMC/SFXP NLT 15 Jan and 15 Jul each year via RCS: HAF-SFI(SA)9222. The report will cover security incidents occurring in the preceding six months and will categorize the incidents as follows. Each security incident must also be annotated to show whether it involved a security violation (compromise/possible compromise) or security infraction. A security "infraction" is any incident that is NOT expected to result in an unauthorized disclosure of classified information.

9.2.7.1. (Added) Unauthorized Access

9.2.7.2. (Added) Mismarking

9.2.7.3. (Added) Unauthorized Transmission

9.2.7.4. (Added) Improper Storage

9.2.7.5. (Added) Unauthorized Reproduction

9.2.7.6. (Added) Improper Classification

9.2.7.7. (Added) Improper Destruction

9.2.7.8. (Added) Other

9.3.1. (Added) To determine the circumstances of occurrence, a preliminary inquiry is immediately initiated into incidents of compromise, possible compromise, or an infraction of the safeguarding controls established by Executive Order 12958 and/or DoD and Air Force   implementing directives. A formal investigation is conducted into complex incidents or those of serious consequence. The servicing ISPM oversees processing of incidents involving collateral classified information, while incidents involving SCI or SAP classified information are handled through those program channels. In addition to the requirements in DoD 5200.1-R, para 10-102, the inquiry or investigation determines:

9.3.1.1. (Added) Whether or not a security incident has occurred.

9.3.1.2. (Added) Appropriate measures or actions to minimize or negate the adverse effect of the security incident.

9.3.1.3. (Added) The seriousness of damage to United States interests.

9.3.1.4. (Added) Appropriate remedial (or corrective) action to prevent the reoccurrence of similar incidents.

9.3.2.1. The unit commander, director or staff agency chief appoints the preliminary inquiry official by the end of the first duty day following discovery. The preliminary inquiry official forwards the preliminary inquiry report to the appointing official within 10 workdays from appointment. The appointing official may grant extensions when fully justified.

9.3.2.3. Coordinate with the Staff Judge Advocate's office to ensure the inquiry is conducted IAW legal requirements. This is particularly important as it relates to interviewing, administering of oaths and the process followed in evaluating information to reach a determination of responsibility for the incident. When these considerations are not present, and the inquiry official is fully experienced in conducting investigations the JAG coordination is optional.

9.3.3. (Added) Preliminary Inquiry.

9.3.3.1. (Added) The servicing ISPM forwards a copy of closed preliminary inquiry reports involving compromise or possible compromise to HQ AFMC/SFXP. Forward these reports within 10 workdays of closure.

9.3.3.2. (Added) A preliminary inquiry establishes that a security infraction or loss or compromise of classified information did not occur; or

9.3.3.3. (Added) That a security infraction occurred constituting a knowing, willful or negligent action contrary to Information Security Program implementing directives, but not involving the loss or compromise of classified information.

9.3.3.4. (Added) That a loss or compromise of classified information did occur but the compromise reasonably could not be expected to cause damage to the national security. If in such instances the official finds no indication of significant security weakness, the report of preliminary inquiry will be sufficient to resolve the incident; or

9.3.3.5. (Added) That the loss or compromise of classified information did occur and that the compromise reasonably could be expected to cause damage to the national security or that the probability of damage to the national security cannot be discounted.

9.3.3.6. (Added) The appointing authority or other designated official notifies the appropriate OCA when there is a loss or compromise of classified information, to include information made public by the news

media. Do not delay this notification pending completion of the inquiry once loss or compromise/potential compromise is confirmed. Notifications revealing that classified information is in the public media is classified at the level of the classified information involved.

9.3.3.7. (Added) When the preliminary inquiry concludes that a security incident has occurred, the report will include a statement categorizing the incident as either a compromise, possible compromise or security infraction (deviation).

9.3.3.8. (Added) An inquiry is not extensive in scope; it gathers available facts to support conclusions or recommendations made by the inquiry official. Upon receipt of the written inquiry report, the appointing authority closes most Air Force information security incidents without opening a formal investigation. This action is based on a determination that no additional substantive information will be obtained by conducting a formal investigation.

9.3.3.9. (Added) When the incident circumstances provide a reasonable expectation of damage to national security, close the inquiry and open a formal investigation.

9.3.4. (Added) Investigations

9.3.4.1. (Added) The unit commander or staff agency chief appoints an investigation official and initiates a formal investigation immediately upon completion of the preliminary inquiry, if warranted by the preliminary inquiry results.

9.3.4.2. (Added) A formal investigation is a detailed and thorough examination of evidence to determine the extent and seriousness of the compromise and to fix responsibility for any disregard (deliberate or inadvertent) of governing directives which led to the security incident.

9.3.4.3. (Added) Investigations include identification of the source, date and circumstances of the compromise; complete description and classification of each item of classified information compromised; a thorough search for the classified information; identification of any person or procedure responsible for the compromise; an analysis and statement of the known or probable damage to the national security that has resulted or may result, and the cause of the loss or compromise; or a statement that compromise did not occur or that there is minimal risk of damage to the national security.

9.3.4.4. (Added) The servicing ISPM monitors and coordinates on reports of investigation.

9.3.4.5. (Added) If not previously accomplished during the preliminary inquiry phase, the appointing authority or other designated official notifies the appropriate OCA when there is a loss or compromise of classified information, to include information made public by the news media. Do not delay this notification pending completion of the investigation once loss or compromise/potential compromise is confirmed. Notifications revealing that classified information is in the public media is classified at the level of the classified information involved.

9.4.1.1. Center Commanders close formal investigations of information security program incidents. This includes security incidents involving classified national security information contained in or processed through automated information systems.

9.5.2. (Added) Damage Assessments.

9.5.2.1. (Added) The OCA, upon learning that a compromise or possible compromise of specific classified information has occurred, and is reasonably expected to cause damage to national security, shall prepare a written damage assessment. While no time limits are placed on completion of the damage assessment, it must be initiated by the OCA upon notification and completed without undue delay. The

OCA must determine whether the damage assessment itself is classified and mark and process accordingly.

9.5.2.2. (Added) As a minimum, damage assessments contain the identification of the source, date and circumstances of the compromise; classification of the specific information lost or compromised; a description of the specific information lost or compromised; an analysis and statement of the known or probable damage to the national security; an assessment of the possible advantages to foreign powers; an assessment of the original classification decision regarding the information involved; and an assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

9.5.2.3. (Added) The OCA notifies all known holders of the information involved if classification levels are changed or the information is declassified.

9.5.2.4. (Added) OCAs must maintain records of damage assessments they prepare in a manner that facilitates their retrieval and use. Dispose of the records IAW records management directives (AFMAN 37-139). OCAs provide a copy of damage assessments to the servicing ISPM for attachment to the file copy of the security incident.

Attachment 3
CONTROLLED UNCLASSIFIED INFORMATION

A3.4.4. (Added) Physical Protection Requirements.

A3.4.4.1. (Added) When not in use, UCNI shall be stored in a manner affording reasonable and adequate protection against unauthorized access. An unlocked container is adequate inside a controlled or guarded area. In other areas, UCNI shall be stored in a locked drawer, desk, repository, or in a locked room.

A3.4.4.2. (Added) UCNI may be reproduced without permission from the originator ONLY to the minimum extent necessary to carry out official duties, and all copies must be marked and protected as the original.

A3.4.4.3. (Added) UCNI shall be disposed of by any approved method of destruction for classified matter, or any other method preventing retrieval.

A3.4.4.4. (Added) UCNI shall be packaged to prevent disclosure of its presence when transmitted by a means that could allow unauthorized access. It will be transmitted by: U.S. First Class, Express, Certified, or registered mail; any means approved for classified; or handcarry by an authorized person maintaining continuous control.

A3.4.4.5. (Added) UCNI may be discussed or transmitted over an unprotected telephone/telecommunications media when required by operational necessity. A more secure means should be used if possible.

Attachment 4

DEPARTMENT OF THE AIR FORCE EXECUTIVE ORDER (EO) 12958 25-YEAR AUTOMATIC DECLASSIFICATION PLAN

A4.6.4. Servicing ISPMs must report the following information concerning local automatic declassification review actions as required by EO 12958, Section 3.4. This information must reach HQ AFMC/SP by the 15th day following the last day of the fiscal quarter (RCS: HAF-SFI(SA)9222 applies):

A4.6.4.1. **(Added)** Baseline holdings:

A4.6.4.2. **(Added)** Number of pages reviewed this period:

A4.6.4.3. **(Added)** Number of pages reviewed to date:

A4.6.4.4. **(Added)** Percent of baseline pages reviewed to date:

A4.6.4.5. **(Added)** Number of pages declassified this period:

A4.6.4.6. **(Added)** Number of pages declassified to date:

A4.6.4.7. **(Added)** Number of pages downgraded this period:

A4.6.4.8. **(Added)** Number of pages downgraded to date:

A4.6.4.9. **(Added)** Number of pages exempted this period:

A4.6.4.10. **(Added)** Number of pages exempted to date:

A4.6.4.11. **(Added)** Exempted pages by category:

A4.6.4.12. **(Added)** -- 25X1 _____

A4.6.4.13. **(Added)** -- 25X2 _____

A4.6.4.14. **(Added)** -- 25X3 _____

A4.6.4.15. **(Added)** -- 25X4 _____

A4.6.4.16. **(Added)** -- 25X5 _____

A4.6.4.17. **(Added)** -- 25X6 _____

A4.6.4.18. **(Added)** -- 25X7 _____

A4.6.4.19. **(Added)** -- 25X8 _____

A4.6.4.20. **(Added)** -- 25X9 _____

A4.6.4.21. **(Added)** TOTAL _____

A4.6.4.22. **(Added)** - Number of referrals to date: _____

A4.6.4.23. **(Added)** - Number of pages referred to date: _____

A4.6.4.24. **(Added)** - Estimated cost for compliance to date: _____

Attachment 7

AFMC ORIGINAL CLASSIFICATION AUTHORITIES

TOP SECRET AUTHORITIES	SECRET AUTHORITIES
HQ AFMC/CC	HQ AFMC/IN
AEDC/CC	AFFTC/CC
AAC/CC	HSC/XR
ASC/CC	DET 1, AFRL/WS
ESC/CC	WR-ALC/LF
OC-ALC/CC	WR-ALC/LK
OO-ALC/CC	WR-ALC/LN
AFRL/CC	WR-ALC/LU
AFRL/DE	WR-ALC/LY
SA-ALC/CC	AAC/WM
WR-ALC/CC	AFRL/MN
SM-ALC/CC	
SMC/CC	
AFRL/IF	
AFRL/ML	
AFRL/SN	
AFRL/VS	

Attachment 8

SECURITY CLASSIFICATION GUIDANCE

A8.1. Program managers having primary management responsibility for a classified weapon system, plan, project, program (including a special access program), operation, equipment, or item (herein referred to as a system) must publish a formal SCG for each system they manage, if not peculiar to and previously published in another SCG. When changes are issued for an SCG, the guide must have a complete review. Identify the next biennial review date as 2 years from the date of the change. Submit DD Form 2024, **DOD Security Classification Guide Data Elements**, RCS: DD-C3I(AR)1418, IAW DoD 5200.1-R, Chapter 2, Section 5, paragraph 2-502; and AFI 31-401, paragraph 2.4. The DD Form 2024 must be signed by a government employee, either military or DoD civilian, of the originating organization or the office of the ISPM.

A8.2. Servicing ISPMs at each installation monitor the biennial review of SCGs issued by activities they service. They send a suspense notice to the 90 days before the review date. The OPR then issues changes as necessary. When major revisions to guides occur, the OPR must review for any change of performance and cost involved for the contractor in relationship to the current DD Form 254, **Contract Security Classification Specification.** Issue a revised DD Form 254, if these changes affect cost and performance. When changes to the basic SCG occur, the country-unique document OPR must evaluate them in order to update the existing document.

A8.3. For SCGs sent to organizations or activities of other Air Force commands, provide a copy to the MAJCOM/SFA office and to HQ AFMC/SFXP.

A8.4. Country-unique security classification documents (guides) developed in support of foreign governments or foreign contractor work performance and approved for release under National Disclosure Policy must contain a statement prohibiting release or disclosure of contents to third countries and their nationals.

A8.5. SCGs are not releasable to foreign nationals or governments except as stated in A2.4 above. Use a DD Form 254 to convey contractual security classification guidance to foreign contractors. For procurement actions with complex security classification considerations, attach only those extracted portions of an approved SCG applicable to the foreign contractual performance to the DD Form 254, provided they are releasable to the foreign government under National Disclosure Policy.

A8.6. Contractor participation in preparation of SCGs is encouraged. However, if more than one contractor is involved in performance of a contract, ensure all have the opportunity to comment and make recommendations for SCG changes.

A8.7. Coordinate all security classification guides, changes, or revisions with the servicing ISPM before publication, except for guides containing sensitive compartmented information (SCI). Also, as appropriate, coordinate guides with the senior intelligence officer (SIO), Public Affairs, Foreign Disclosure, OPSEC and COMSEC officers.

A8.8. Use one classification designation, e.g., U, C, S, or TS, under the classification column. Do not use U-TS, C-S etc. This forces the reader to make an original classification decision. Explain any differences in classification in the remarks column. The remarks column clarifies classification guidance when required.

A8.9. The servicing ISPM classification management specialist keeps on file:

- A current DoD 5200.1-R and DOD 5200-1H.
- One copy of classification guides (and changes/revisions) issued by activities they service
- Related DD Forms 2024.
- Other SCGs necessary to support activities serviced.

A8.10. See basic regulation, paragraphs 2-400, 5-206c and 5-302, for further guidance on applying the compilation rule and proper marking of documents.

A8.11. The reason for assignment of distribution statements on the cover page for SCGs may be either Critical Technology or Specific Authority. Add distribution (AFI 61-204, *Disseminating Scientific and Technical Information*), reproduction limitation and destruction statements, as applicable, to guides. Deny FOIA requests for guides or unclassified extracts of classified guides according to 5 USC 552 (B)(2).

A8.12. OCA signature is required on the "Foreword" page of the SCG. Record copy reflects OPR/program manager and servicing ISPM coordination.

A8.13. Review distribution list upon revisions to SCGs to ensure only activities requiring SCGs are identified.

A8.14. Revised SCGs and changes must contain a summary of changes, to include the topic or item changed. An OCA must approve and sign changes to guides involving classification decisions.

Attachment 9

SAMPLE TRAINING PLAN (ACTIVITY)

A9.1. References:

  a. DoDD 5000.1, *Defense Acquisition, para D.1.e*

  b. DOD 52OO.l-R, *Information Security Program Regulation*

  c. DOD 5200-1-PH, *A Guide To Marking Classified Documents*

  d. DoD 5200.1M, *Acquisition Systems Protection Program/AFI 31-701*

  e. DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*

  f**.** AFI 10-1101, *Operations Security (OPSEC) Instructions*

  g. AFI 31-209, *The Air Force Resource Protection Program*

  h. AFI 31-210, *The Air Force Antiterrorism (AT) Program*

  i. AFI 31-402, *Applying North Atlantic Treaty Organization (NATO) Protection Standards (pending)*

  j. AFI 31-403, *Security Education Training and Awareness (pending)*

  k. AFI 31-404, *USAF Security Classification Guide Database (pending)*

  l. AFH 31-405, *USAF Information Security Program (pending)*

  m. AFI 31-501, *Personnel Security Program Management*

  n. AFI 31-601*, Industrial Security Program Management*

  o. AFI 61-204, *Disseminating Scientific and Technical Information*

  p. AFI 61-205, *Sponsoring or Co-Sponsoring, Conducting, and Presenting DOD-Related Scientific Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings*

  q. AFI 71-101V1 and V2, *Criminal Investigations, Counterintelligence, and Protective Service Matters*

  r. Executive Order 12958, *Classified National Security Information*

  s. AFKAG 1, *COMSEC Responsibilities*

A9.2. General. Commanders, staff agency chiefs and supervisors must ensure personnel understand the compelling need to protect classified and sensitive information, material and systems. To accomplish this, they ensure their personnel receive training as follows. All training areas may be expanded as determined locally: Initial Security Training is provided within 10 work days of a person physically assuming a position. This training will, as a minimum, cover subjects listed in DoD 5200.1-R, paragraph 9-200 and related subparagraphs. Special Requirements Training, as prescribed in DoD 5200.1-R, Chapter 9, Section 3, is presented within 30 days of an individual assuming a qualifying position. Security managers may present this training Thereafter, security managers provide Recurring and Refresher training. As a minimum, this training must be presented on a semi-annual basis, but quarterly sessions are recommended. Training via automated systems is the desired approach.

A9.3. Schedule (Quarterly Recurring/Refresher Training).

a. **First session.**

(1) Security Program Roles and responsibilities

(2) Elements of classifying and declassifying information

(3) Elements of safeguarding

(4) Original classifiers' responsibilities and Classification Principles

(5) Declassification Standards and Methods

b. **Second session.**

(1) Original and derivative classification processes

(2) Classification markings

(3) Authorities, methods and processes for downgrading and declassifying information

(4) Methods for proper use, storage, reproduction, transmission, dissemination anddestruction of classified information

(5) Responsibilities of personnel serving as couriers of classified information.

c. **Third session.**

(1) Requirements for creating and updating classification/declassification guides

(2) Requirements for controlling access to classified information

(3) Procedures for investigating and reporting instances of security violations

(4) Sanctions for violating security directives/laws

(5) Protecting classified information stored in automated information systems

(6) Philosophies, requirements, and techniques embodied in the Industrial Security Program.

d. **Fourth session.**

(1) Requirements for creating, maintaining, and terminating special access programs

(2) Mechanisms for monitoring special access programs

(3) Practices applicable to U.S. officials traveling overseas

(4) Requirements for oversight of the security classification program, including self inspections

(5) The threat and techniques employed by foreign intelligence activities attempting to obtain classified information.

APPROVED

_____   _____

Commander/Staff Agency Chief Signature   Date

                          HUBERT G. MITCHELL, Colonel, USAF
                          Director, Security Forces